FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1419242-000

Total Deleted Page(s) = 7
Page 8 ~ b3; b6; b7C; b7E;
Page 9 ~ b6; b7C; b7E;
Page 13 ~ Duplicate;
Page 15 ~ Duplicate;
Page 16 ~ Duplicate;
Page 19 ~ Duplicate;
Page 20 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/23/2010

To: Indianapolis **Attn:** Evidence

Newark **Attn:** Cyber Investigations
SA

b3
b6
b7C
b7E

From: Indianapolis
C3
Contact: SA

Approved By:

Drafted By: C3\296 01.ec)

Case ID #: -55 (Pending)

Title: ET AL;
D/B/A/GOATSE SECURITY
COMPUTER INTRUSION - CRIMINAL

Synopsis: Evidence transfer.

Package Copy: Being forwarded under separate cover is 1B39 Barcode E4609324.

Details: At the request of Newark Division, evidence item 1B39, which was collected by Indianapolis Division is to be transferred to from Indianapolis to Newark.

UNCLASSIFIED

-55

To: Indianapolis From: Indianapolis
Re: [redacted] 10/23/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

NEWARK

AT SOMERSET, NJ

Read and clear.

♦♦

ORIGINAL FILE COPY

Do not write on or otherwise alter these documents.

Return the attached documents to your SST upon completion to be refiled into the substantive case file.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/26/2010

To: Newark

From: Newark
FT2/FTRA
Contact: SA [redacted] b6 b7C

Approved By: [redacted] b3 b7E

Drafted By: [redacted]

Case ID #: [redacted] (Pending) -56

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: To document search warrant extension(s) granted by the Northern District of California, relating to evidence seized on July 26, 2010, at [redacted] b6 b7C

Details: On October 25, 2010, Honorable Joseph C. Spero, United States Magistrate Judge, in the Northern District of California, San Jose Division, granted an extension for evidence seized on July 26, 2010, at [redacted]

In summary and in part, the court order granted a 60 day extension for [redacted] A complete list of [redacted] b7E are further listed by item description in the court order.

The court order further granted a 120 day extension for [redacted] A complete list of [redacted] are b7E further listed by item description in the court order.

Copy of the signed court order is enclosed in the attached FD-340 envelope which will be maintained in the evidentiary (1A) section of the substantive case file.

♦♦

UNCLASSIFIED

[redacted]

b3
b6
b7C
b7E

02:08 pm Initial appearance began.

02:30 pm Initial appearance proceedings end. [redacted] is detained pending a detention hearing scheduled for Friday 1/21/2011 at 9am before Honorable Erin Setser

Original fingerprints and photographs of [redacted] along with United States Marshals Service form USM-129, and arrest log notes are enclosed in an FD-340 envelope which will be maintained in the evidentiary (1A) section of the substantive case file.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/01/2010

[redacted] date of birth [redacted] was interviewed telephonically. [redacted] resides at [redacted] telephone number is [redacted] email address is [redacted] After being advised of the identity of the interviewing agents, and the nature of the interview, [redacted] provided the following information: b6 b7C

[redacted] Dreamwidth Studios, LLC doing business as www.dreamwidth.org. [redacted] explained Dreamwidth Studios, LLC ("Dreamwidth") is a social media journaling forum much like LiveJournal, where users share common interests. [redacted] used the open source code from LiveJournal, to create Dreamwidth. b6 b7C

Dreamwidth was registered in April 2008, and available to the public in approximately February 2009. Dreamwidth consists of about 80 percent volunteers, and is user supported. A basic account costs $35 per year and $50 per year for a premium account. Dreamwidth previously used IRC channel #dw on irc.dwscoalition.org but has moved to #dreamwidth on irc.freenode.net.

[redacted] became the attention of an internet hacking group, known as "BANTOWN". [redacted] stated BANTOWN began conducting unsolicited security audits against the LiveJournal website. [redacted] stated BANTOWN was able to obtain login information for multiple LiveJournal accounts using a "cross-site scripting" attack. [redacted] stated [redacted] created a website [redacted] stated [redacted] posted several articles on a forum "Full Disclosure" [redacted] b6 b7C

Investigation on 12/1/2010 at Somerset, NJ (telephonically)

File # [redacted]-59 Date dictated 12/1/2010

by SA [redacted]
SA [redacted]

b6 b7C b3 b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

b6
b7C
b3
b7E

[redacted]

In January 2010 members of the GNAA created a group called "Parents for Responsible New Media", in order to bring pressure against Dreamwidth for allegations of hosting child pornography. GNAA used this new group as a way to contact PayPal and Google Checkout, claiming that Dreamwidth was involved in child pornography, to put pressure on the online merchants to discontinue service with Dreamwidth. On January 8, 2010 PayPal shut down Dreamwidth's account. On February 18, 2010, Google Checkout shut down Dreamwidth's account.

[redacted] stated in January 2010 they also experienced a Denial of Service Attack (DOS) against their website resulting in a degradation in website performance, and for some users the entire website was offline. [redacted] stated their hosting provider, SERVERBEACH, did not charge any additional bandwidth charges as a result of the DOS attack. The DOS attack lasted approximately 72 hours. [redacted] stated to her knowledge, SERVERBEACH, was unable to determine the source of the DOS attack.

[redacted] stated, [redacted] and her email address is [redacted] residing in [redacted] was monitoring IRC chats in a GNAA IRC channel. [redacted] stated [redacted] observed [redacted] chatting about actions he and other members of the GNAA had taken against Dreamwidth. [redacted] posted a document containing employment records, home addresses, and contact information for volunteer members of Dreamwidth. In IRC chats, [redacted] incited other GNAA members to "take action" against volunteer members of Dreamwidth.

[redacted] stated there are several recorded conversations between members of GNAA and members of Dreamwidth, that were streamed over the Internet. [redacted] stated on at least one occasion, she was able to listen to the streamed audio, as the conversation was being recorded real time.

On or about January 14, 2010, [redacted] Dreamwidth, was targeted by GNAA and multiple reports were made to Child Services claiming [redacted] was a child pedophile. [redacted] stated [redacted] was interviewed by Child Services, with negative results.

When [redacted] was asked about knowledge of the AT&T iPad 3G attack, she responded that she had no information or knowledge of the attack other than what was publicly available in the media.

When [redacted] was asked if Dreamwidth saved IRC chat logs she responded, "No, not officially but some members of Dreamwidth save copies of the logs from when they are connected to the IRC channel".

When [redacted] was asked if she was ever contacted by Goatse Security or a member of Goatse Security, she responded, "Never contacted by Goatse Security. Best guess among members of the security community is that Goatse Security was created in mid 2010, for the sole purpose of the AT&T/Apple attack".

[redacted] stated she has never visited the Goatse Security website, although she is familiar with the meaning of the Goatse Security logo and the image that has been passed around the Internet. [redacted] stated other than [redacted] and his public statements of affiliation with Goatse Security, she does not know any of the other members.

Dreamwidth was able to find a new online bill pay merchant, in April 2010. [redacted] estimated that between January 2010 and April 2010, Dreamwidth lost $50,000 in subscription revenue because their online merchants closed their accounts, due to the harassment from GNAA.

[redacted] prepared a written statement of fact, which was emailed to SA [redacted] and has a DVD of supporting evidence and copies of IRC chats, referenced in the statement of fact. SA [redacted] requested that [redacted] mail a signed her statement, and any supporting evidence or documentation to the Franklin Township Resident Agency, for review. [redacted] stated she would cooperate with law enforcement in any way possible.

The email from [redacted] dated 12/1/2010, and her statement of fact are enclosed in an FD-340 envelope which will be maintained in the evidentiary (1A) section of the substantive case file.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/18/2011

Pursuant to the execution of an authorized federal arrest warrant issued 01/13/2011 by the United States District Court, District of New Jersey, and signed by the Honorable CLAIRE CECCHI United States Magistrate Judge, on 01/18/2011 Special Agents (SA) of the Federal Bureau of Investigation (FBI) effected the arrest of [redacted] at the Washington County Court House, 280 N. College Ave, Fayetteville, Arkansas. Present during the execution of the arrest were SA [redacted] and SA [redacted] All of the below listed times are approximate, and in recorded Central Time: b6 b7C

07:43 am [redacted] taken into custody without incident and searched incident to arrest in the 4th floor waiting area of the Washington County Court House.

07:45 am [redacted] requested to make a call to [redacted] and was permitted. b6 b7C

07:55 am [redacted] requested to make a call to [redacted] and was permitted.

08:04 am [redacted] met with his attorney, [redacted] in a conference room on the 4th floor of the courthouse.

08:50 am [redacted] was transferred to the custody of Washington County Deputy Sheriff, [redacted] badge# [redacted] for transport to the Washington County Jail.

12:26 pm SA [redacted] and SA [redacted] remand [redacted] to FBI custody from the Washington County Jail, for transport to initial appearance.

12:30 pm SA [redacted] and SA [redacted] departed Washington County Jail, starting mileage: 69, 369

12:36 pm SA [redacted] and SA [redacted] arrived at United States Marshal's service, ending mileage: 69, 372, custody of [redacted] transferred to Marshal's custody pending initial appearance at 2:00 pm.

Investigation on 01/18/2011 at Fayetteville, AR

File # [redacted]-60 Date dictated N/A

by SA [redacted] b6 b7C b3 b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Record Request
FD-125 (Rev. 4-1-93)

Date 10/20/2010

b6
b7C
b3
b7D

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

To	Buded
Return	File Number 59

Name and aliases of subject, applicant, or employee, and spouse

Address
Residence
Business
Former

* Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☐ Female ☐ Male					

Birth date	Birthplace	
Arrest Number	Fingerprint classification	Criminal specialty

Social Security Number	Divers License Number ☐ D/L Photo ☐ Other

Specific information desired
full background

Results of check

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1419242-000

Total Deleted Page(s) = 34
Page 1 ~ OTHER - Sealed Per Court Order;
Page 2 ~ OTHER - Sealed Per Court Order;
Page 3 ~ OTHER - Sealed Per Court Order;
Page 4 ~ OTHER - Sealed Per Court Order;
Page 5 ~ OTHER - Sealed Per Court Order;
Page 6 ~ OTHER - Sealed Per Court Order;
Page 7 ~ OTHER - Sealed Per Court Order;
Page 8 ~ OTHER - Sealed Per Court Order;
Page 9 ~ OTHER - Sealed Per Court Order;
Page 10 ~ OTHER - Sealed Per Court Order;
Page 11 ~ OTHER - Sealed Per Court Order;
Page 12 ~ OTHER - Sealed Per Court Order;
Page 13 ~ OTHER - Sealed Per Court Order;
Page 14 ~ OTHER - Sealed Per Court Order;
Page 15 ~ OTHER - Sealed Per Court Order;
Page 16 ~ OTHER - Sealed Per Court Order;
Page 17 ~ OTHER - Sealed Per Court Order;
Page 18 ~ OTHER - Sealed Per Court Order;
Page 19 ~ OTHER - Sealed Per Court Order;
Page 20 ~ OTHER - Sealed Per Court Order;
Page 21 ~ OTHER - Sealed Per Court Order;
Page 22 ~ OTHER - Sealed Per Court Order;
Page 23 ~ OTHER - Sealed Per Court Order;
Page 24 ~ OTHER - Sealed Per Court Order;
Page 25 ~ OTHER - Sealed Per Court Order;
Page 26 ~ OTHER - Sealed Per Court Order;
Page 27 ~ OTHER - Sealed Per Court Order;
Page 28 ~ OTHER - Sealed Per Court Order;
Page 36 ~ Duplicate;
Page 37 ~ Duplicate;
Page 38 ~ Duplicate;
Page 39 ~ Duplicate;
Page 40 ~ Duplicate;
Page 43 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/19/2010

To: Newark **Attn:** Newark

From: Newark
FT2
Contact: SA [redacted] b6 b7C

Approved By: [redacted] b3 b7E

Drafted By: [redacted]

Case ID #: [redacted] -54

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: To document return phone call to [redacted] b6 b7C regarding evidence seized during a Federal Search Warrant on June 15, 2010.

Details: [redacted] contacted the Little Rock FBI Field Office on October 18, 2010 inquiring as to when, "she can get her stuff back" that was seized during the execution of a Federal Search Warrant at her residence on June 15, 2010.

On October 19, 2010 at approximately 2:38pm, writer contacted [redacted] at [redacted], and informed her that her items seized during the search are still being reviewed and considered evidence. If and when they can be cleared as evidence, arrangements will be made to return those items. [redacted] was provided the main office number for the Newark FBI Field Office, if she has further questions.

♦♦

UNCLASSIFIED

To: Newark From: [redacted] b3
Re: [redacted] 09/09/2010 b7E

LEAD(s):

Set Lead 1: (Info)

NEWARK

AT NEWARK

Read and clear.

♦♦

FD-302 (Rev. 10-6-95)

FBI Newark

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/23/2010

A physical surveillance was conducted in the vicinity of [redacted] During the surveillance activity, the following observations were made at the appropriate time noted: b6 b7C

Time	Observations
8:10 am	Surveillance initiated.
	[redacted]
10:10 am	
12:00 pm	Surveillance terminated.

Notes taken during the surveillance activity are placed in the 1A portion of this case file.

Investigation on 07/19/2010 at San Francisco, California

File # [redacted]-45 Date dictated Not Dictated

by SAs [redacted] b6 b7C b3 b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2010

On 07/27/2010, pursuant to an authorized search warrant signed on 07/26/2010 by United States Magistrate Marie-Elena James, Northern District of California, Special Agents (SA) of the FBI executed a search warrant at [redacted] at approximately 7:01 AM Pacific Daylight Time. The SAs and associated duties are listed as follows: b6 b7C

[redacted] Supervisory Special Agent, Entry b6 b7C
[redacted] Entry and Search
[redacted] Entry and Search
[redacted] Entry, Search Team Leader
[redacted] Entry, Search
[redacted] Search
[redacted] Search
[redacted] Search
[redacted] Search
[redacted] Case Agent, Search, Interviewer
[redacted] Co-Case Agent, Search, Interviewer

At approximately 7:01 AM PDT, SA [redacted] conducted a knock and announce at [redacted] After approximately 30 seconds, [redacted] date of birth [redacted] opened the door to the apartment. [redacted] was briefly detained while agents conducted a protective sweep of the residence. b6 b7C

Once the protective sweep was completed and the residence deemed clear, [redacted] was told by the agents present the FBI was executing a search warrant and that he was not under arrest. He was further advised that he was free to leave the premises at any time. [redacted] elected to stay in the residence and thus was advised that he could not move about freely in the apartment without an agent escort while the search warrant was being executed. [redacted] agreed to these terms. [redacted] was shown a copy of the search warrant. b6 b7C

Initial inspection of the apartment unit found it to be a [redacted]

Investigation on 07/27/2010 at San Francisco, CA b6 b7C

File # [redacted] -46 Date [redacted] No Dictati[redacted] b3 b7E

SAs

by [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

At approximately 7:06 AM PDT, another resident of returned to the residence under the escort of SA This resident was identified from his driver's license as:

Name:
DOB:
Race:
Sex:
Address:

Cell Phone:

advised he was At approximately 7:08 AM PDT, after providing his identification, stated he needed to go to work and subsequently left the premises.

At approximately 7:08 AM PDT, entry photos were taken and a formal search began.

At approximately 7:31 AM PDT, forensic examiners (FE) from the Silicon Valley Regional Computer Forensic Laboratory (SVRCFL) and Task Force Officer (TFO) FEs and arrived at the premises to inspect the computers in the bedroom. FE entered the premises at approximately 8:50 AM PDT to provide assistance.

[redacted]

b6
b7C
b3
b7E

During the search, SAs [redacted] and [redacted] began interviewing [redacted] (refer to interview FD-302). The SVRCFL FEs began imaging [redacted] Photographs of evidence were taken as appropriate.

At approximately 8:21 AM PDT, SAs [redacted] and [redacted] left the premises. At approximately 9:03 AM PDT, SSA [redacted] left the premises.

Beginning approximately 11:20 AM PDT, exit photos of the apartment were taken. During this time, [redacted] was presented with copies of the FD-597 documenting items being seized from the residence. A photograph was taken of [redacted] holding the FD-597 receipts and a copy of the search warrant. [redacted] was told the [redacted]

At approximately 11:40 AM PDT, the search was formally completed and control of the apartment unit was returned to [redacted] closed and locked the door as agents left.

The following items were seized from the premises:

[redacted]

[redacted]

[redacted]

b6
b7C
b3
b7E

Photographs were taken by SA [redacted] with corresponding photo logs recorded by SA [redacted] A sketch, not drawn to scale, was made by SA [redacted] Evidence Recovery log and Finder duties were performed by SA [redacted] and SA [redacted] Evidence was transported to the evidence control room at the Oakland Resident Agency of the FBI.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/15/2010 b6 b7C

To: Newark **Attn:** SA [redacted]
Squad FT2

From: San Francisco
Squad CY1/Hayward RA
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted] b3 b7E

Case ID #: [redacted] (Pending) -47

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: To cover lead #1 set in referenced communication.

Reference: [redacted] Serial 34

Enclosure(s): Enclosed for Newark are the following:
1) FD-302 and copy documenting search warrant execution at [redacted]
2) FD-340 envelope containing administrative log, sketch, digital photos on CD, photo log, evidence recovery log, copy of search warrant return, original FD-888 ops plan, and FD-597; b3 b6 b7C b7E
3) FD-302 and copy documenting surveillance of [redacted]

Details: Per referenced communication, Newark requested San Francisco to verify residence of [redacted] hereafter referred to as "Premises", and then conduct search warrant execution at the above listed address.

on 07/27/2010, after confirming [redacted] resided at the Premises, San Francisco executed a search warrant at the Premises. [redacted] was home and items were seized as documented in the enclosed FD-302 documents. San Francisco considers lead number 1 in referenced communication covered.

♦♦

UNCLASSIFIED

CORE
SF-175 41

288A-NK-118470 -47

FD-302 (Rev. 10-6-95)

b6
b7C
b7D

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/06/2010

Special Agent [redacted] observed [redacted] copy [redacted] to a 4GB Centon USB drive provided by [redacted] who is detailed to the FBI Cyber Crime Task Force. The contents were copied to a folder labeled [redacted] The USB drive was provided to [redacted]

b6
b7C
b7D
b7E

Subsequent to the file copying, [redacted] provided SA [redacted]

[redacted]

b7D

A copy of the consent to search authorization documents completed by [redacted] and the document bearing [redacted] were placed into the 1A section of the case file. The cd-rom disk obtained from [redacted] was placed into evidence.

Investigation on 10/06/2010 at Indianapolis, Indiana

File # [redacted] - 48 Date dictated 10/06/2010

by SA [redacted] (C3\279[redacted]01.302)

b6
b7C
b3
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

b6
b7C
b7E

Precedence: DEADLINE 11/12/2010 **Date:** 10/15/2010

To: Operational Technology **Attn:**

Newark **Attn:** FTRA 2
SA
SA

From: Newark
NJRCFL
Contact:

Approved By:

Drafted By:

Case ID # Pending) -4849
(Pending)

b3
b7E

Title:
COMPUTER INTRUSION

b6
b7C

b6
b7C
b7E

Synopsis: Request

Administrative: Per telcal on 08/24/2010 between and NK-NJRCFL, regarding the submission of items from NJRCFL-10-387.

Package Copy: Being forwarded under separate cover is the evidence listed below, via FedEx Tracking number 8718 0441 3698.

Enclosure(s): One (1) copy of Search Warrant dated 7/26/2010 issued in United States District Court for the Northern District of California, one (1) Report of Examination dated 10/15/2010 by FE that are more particularly described below.

UNCLASSIFIED

b6
b7C

To: Operational Technology From: Newark
Re: [redacted] 10/15/2010

b7E
b3

Details: The enclosed items listed below were seized in captioned matter from a subject residing in San Francisco, California. Evidence was seized and transported to the Newark division and is in need of a forensic examination. [redacted]

[redacted]

It should be noted, seizure took place in the 9th Circuit and as such, additional speedy processing requirements exist. Post-CDT requirements in that district require agents to image/process the seized evidence within 30 days of seizure and examine images no later than 120 days. The legal authority for this request will be provided along with the items listed below. It is requested that the items be processed and the results supplied to the New Jersey Regional Computer Forensic Laboratory, 1200 Negron Drive, Hamilton, New Jersey, 08691.

b7E
b6
b7C

[redacted]

[redacted] Provide results. Need before 120 day order by Judge.

To: Operational Technology From: Newark
Re: [redacted] 10/15/2010

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA

b7E
b3

[redacted] and provide results.

Set Lead 2: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA

Provide status update prior to EC Deadline of 11/15/2010 to NJRCFL, [redacted]

b6
b7C

Set Lead 3: (Info)

NEWARK

AT FRANKLIN TOWNSHIP RA

Read and clear.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 11/12/2010 **Date:** 10/18/2010

To: Operational Technology **Attn:**

Newark **Attn:** FTRA 2
SA
SA

From: Newark
NJRCFL
Contact: b6 b7C

Approved By:

Drafted By:

Case ID #: (Pending) -50
(Pending) b3 b7E

Title: b6 b7C
COMPUTER INTRUSION
b6 b7C b7E

Synopsis: Request b7E

Administrative: Per telcal on 08/24/2010 between b6 b7C
and NK-NJRCFL, regarding the submission of items b7E

Package Copy: Being forwarded under separate cover is the evidence listed below, via FedEx Tracking number 8718 0441 3665.

Enclosure(s): One (1) copy of Search Warrant dated 7/26/2010 issued in United States District Court for the Northern District of California, one (1) Report of Examination dated 10/18/2010 by FE that are more particularly described below.

Details: The enclosed items listed below were seized in captioned matter from a subject residing in San Francisco, California. Evidence was seized and transported to the Newark

UNCLASSIFIED

b6
b7C

To: Operational Technology From: Newark
Re: [redacted] 10/18/2010

division and is in need of a forensic examination. The media within this request [redacted] b7E b3

It should be noted, seizure took place in the 9th Circuit and as such, additional speedy processing requirements exist. Post-CDT requirements in that district require agents to image/process the seized evidence within 30 days of seizure and examine images no later than 120 days. The legal authority for this request will be provided along with the items listed below. It is requested that the items be processed and the results supplied to the New Jersey Regional Computer Forensic Laboratory, 1200 Negron Drive, Hamilton, New Jersey, 08691.

[redacted] b6 b7C b7E

[redacted] Provide results. Need before 120 day order by Judge.

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA b7E

[redacted] and provide results.

Set Lead 2: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA

Provide status update prior to EC Deadline of 11/15/2010 to NJRCFL, [redacted]. b6 b7C b7E

To: Operational Technology From: Newark
Re: [redacted] 10/18/2010

b3
b7E

Set Lead 3: (Info)

NEWARK

AT FRANKLIN TOWNSHIP RA

Read and clear.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

b6
b7C
b7E

Precedence: DEADLINE 11/12/2010 **Date:** 10/18/2010

To: Operational Technology **Attn:**

Newark **Attn:** FTRA 2
SA
SA

From: Newark
NJRCFL
Contact:

b6
b7C
b7E

Approved By:

Drafted By:

Case ID #: (Pending) -51
(Pending)

b3
b7E

Title:
COMPUTER INTRUSION

b6
b7C

Synopsis: Request

b7E

Administrative: Per telcal on 08/24/2010 between and NK-NJRCFL, regarding the submission of items

Package Copy: Being forwarded under separate cover is the evidence listed below, via FedEx Tracking number 8718 0441 3665.

b6
b7C
b7E

Enclosure(s): One (1) copy of Search Warrant dated 7/26/2010 issued in United States District Court for the Northern District of California, one (1) Report of Examination dated 10/18/2010 by FE that is more particularly described below.

Details: The enclosed items listed below were seized in captioned matter from a subject residing in San Francisco, California. Evidence was seized and transported to the Newark division and is in need of a forensic examination. The enclosed

UNCLASSIFIED

b6
b7C

To: Operational Technology From: Newark
Re: [redacted] 10/18/2010

[redacted] b7E b3

It should be noted, seizure took place in the 9th Circuit and as such, additional speedy processing requirements exist. Post-CDT requirements in that district require agents to image/process the seized evidence within 30 days of seizure and examine images no later than 120 days. The legal authority for this request will be provided along with the items listed below. It is requested that the items be processed and the results supplied to the New Jersey Regional Computer Forensic Laboratory, 1200 Negron Drive, Hamilton, New Jersey, 08691.

[redacted] b6 b7C b7E

[redacted] Provide results. Need before 120 day order by Judge.

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA b7E

[redacted] and provide results.

Set Lead 2: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA

To: Operational Technology From: Newark
Re: [redacted] 10/18/2010

Provide status update prior to EC Deadline of 11/15/2010 to NJRCFL, [redacted]

b6
b7C
b3
b7E

Set Lead 3: (Info)

NEWARK

AT FRANKLIN TOWNSHIP RA

Read and clear.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 11/12/2010 **Date:** 10/15/2010

To: Operational Technology **Attn:** [redacted]

Newark **Attn:** FTRA 2
SA [redacted]
SA [redacted]

From: Newark
NJRCFL
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) -52
[redacted] (Pending)

Title: [redacted]
COMPUTER INTRUSION
[redacted]

Synopsis: Request [redacted]

Administrative: Per telcal on 08/24/2010 between [redacted] and NK-NJRCFL, [redacted] regarding the submission of items [redacted] from NJRCFL-10-387.

Package Copy: Being forwarded under separate cover is the evidence listed below, via FedEx Tracking number 8718 0441 3698.

Enclosure(s): One (1) copy of Search Warrant dated 7/26/2010 issued in United States District Court for the Northern District of California, one (1) Report of Examination dated 10/15/2010 by FE [redacted] that is more particularly described below.

Details: The items listed below were seized in captioned matter from a subject residing in San Francisco, California. Evidence was seized and transported to the Newark division and is in need of a forensic examination. The enclosed hard drive contains

UNCLASSIFIED

[redacted]

To: Operational Technology From: Newark
Re: [redacted] 10/15/2010

[redacted] b7E b3

It should be noted, seizure took place in the 9th Circuit and as such, additional speedy processing requirements exist. Post-CDT requirements in that district require agents to image/process the seized evidence within 30 days of seizure and examine images no later than 120 days. The legal authority for this request will be provided along with the items listed below. It is requested that the items be processed and the results supplied to the New Jersey Regional Computer Forensic Laboratory, 1200 Negron Drive, Hamilton, New Jersey, 08691.

[redacted] b6 b7C b7E

[redacted] Provide results. Need before 120 day order by Judge.

To: Operational Technology From: Newark
Re: [redacted] 10/15/2010

LEAD(s):

Set Lead 1: (Action)

b7E
b3

OPERATIONAL TECHNOLOGY

AT [redacted] QUANTICO, VA

[redacted] and provide results.

Set Lead 2: (Action)

OPERATIONAL TECHNOLOGY

AT [redacted], QUANTICO, VA

Provide status update prior to EC Deadline of 11/15/2010 to NJRCFL, [redacted]

b6
b7C

Set Lead 3: (Info)

NEWARK

AT FRANKLIN TOWNSHIP RA

Read and clear.

♦♦

Record Request
FD-125 (Rev. 4-1-93)

Date 3/10/2010

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

b6
b7C
b3
b7E

To [redacted]

Buded

Return [redacted]

File Number [redacted] -53

Name and aliases of subject, applicant, or employee, and spouse

[redacted]

Address

Residence _____

Business _____

Former _____

* Date and place of marriage (if applicable) _____

Race	Sex	Age	Height	Weight	Hair	Eyes
	☐ Female ☐ Male					

Birth date | Birthplace

Arrest Number | Fingerprint classification | Criminal specialty

Social Security Number | Divers License Number ☐ D/L Photo ☐ Other

Specific information desired: full background

Results of check

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/09/2010

To: Newark **Attn:** SA

From:
CY-1
Contact: SA

Approved By:

Drafted By:

Case ID #: (Pending) -44

Title: ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b6
b7C
b3
b7E

GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(e)

Synopsis: To cover lead in response to service of Federal Grand Jury (FGJ) Subpoena.

Reference: Serial 39

Enclosure(s): Original executed copy of FGJ Return of Service.

Details: On 08/20/10 at approximately 6:15 PM, writer and Special Agent (SA) served referenced FGJ Subpoena to at his residence at

b3
b6
b7C

On 08/23/10, the enclosure was scanned and emailed to SAs and The enclosure considers lead covered.

UNCLASSIFIED

b6
b7C

25 01. WPD

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1419242-000

Total Deleted Page(s) = 80
Page 21 ~ Duplicate;
Page 22 ~ Duplicate;
Page 23 ~ Duplicate;
Page 24 ~ Duplicate;
Page 25 ~ Duplicate;
Page 29 ~ Duplicate;
Page 34 ~ Duplicate;
Page 35 ~ Duplicate;
Page 36 ~ Duplicate;
Page 39 ~ Duplicate;
Page 40 ~ Duplicate;
Page 46 ~ b3; b6; b7C; b7D; b7E;
Page 51 ~ Duplicate;
Page 52 ~ Duplicate;
Page 53 ~ Duplicate;
Page 54 ~ Duplicate;
Page 58 ~ Duplicate;
Page 60 ~ b3; b6; b7C; b7E;
Page 61 ~ b7E;
Page 62 ~ b6; b7C; b7E;
Page 64 ~ b6; b7C; b7E;
Page 65 ~ b7E;
Page 66 ~ b6; b7C;
Page 67 ~ b7E;
Page 68 ~ b7E;
Page 69 ~ b7E;
Page 70 ~ Duplicate;
Page 77 ~ b3; b6; b7C; b7D; b7E;
Page 78 ~ b3; b7E;
Page 79 ~ b3; b6; b7C; b7D; b7E;
Page 80 ~ b3; b7E;
Page 81 ~ Duplicate;
Page 82 ~ Duplicate;
Page 86 ~ Duplicate;
Page 87 ~ Duplicate;
Page 88 ~ Duplicate;
Page 91 ~ b3; b6; b7C; b7E;
Page 92 ~ b3; b6; b7C; b7E;
Page 93 ~ b3; b6; b7C; b7E;
Page 96 ~ b3; b6; b7C; b7D; b7E;
Page 98 ~ b3; b6; b7C; b7D; b7E;
Page 99 ~ b3; b6; b7C; b7D; b7E;
Page 100 ~ b3; b6; b7C; b7D; b7E;
Page 101 ~ b3; b6; b7C; b7D; b7E;
Page 102 ~ b3; b6; b7C; b7D; b7E;
Page 107 ~ b3; b6; b7C; b7E;
Page 108 ~ b6; b7C; b7E;
Page 109 ~ b6; b7C; b7E;
Page 110 ~ b6; b7C; b7E;
Page 111 ~ b6; b7C; b7E;
Page 112 ~ b6; b7C; b7E;
Page 113 ~ b6; b7C; b7E;
Page 114 ~ b6; b7C; b7E;
Page 118 ~ Duplicate;
Page 119 ~ Duplicate;
Page 122 ~ b3; b6; b7C; b7E;
Page 123 ~ b6; b7C; b7E;
Page 124 ~ b6; b7C; b7E;
Page 125 ~ b6; b7C; b7E;
Page 126 ~ b6; b7C; b7E;
Page 127 ~ b6; b7C; b7E;
Page 128 ~ b7E;
Page 129 ~ b6; b7C; b7E;
Page 130 ~ b6; b7C; b7E;
Page 131 ~ b6; b7C; b7E;
Page 132 ~ b6; b7C; b7E;
Page 133 ~ b6; b7C; b7E;

Page 134 ~ b6; b7C; b7E;
Page 135 ~ b6; b7C; b7E;
Page 136 ~ b6; b7C; b7E;
Page 138 ~ Duplicate;
Page 142 ~ Duplicate;
Page 143 ~ OTHER - Sealed per Court Order;
Page 144 ~ OTHER - Sealed per Court Order;
Page 145 ~ OTHER - Sealed per Court Order;
Page 146 ~ OTHER - Sealed per Court Order;
Page 147 ~ OTHER - Sealed per Court Order;
Page 148 ~ OTHER - Sealed per Court Order;
Page 149 ~ OTHER - Sealed per Court Order;
Page 150 ~ OTHER - Sealed per Court Order;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/10/2010

To: Newark **Attn:** [redacted]
Victim Specialist

Cyber **Attn:** CCS, CCU-2
SSA [redacted]

From: Newark
FT2
Contact: SA [redacted] b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] b3 b7E

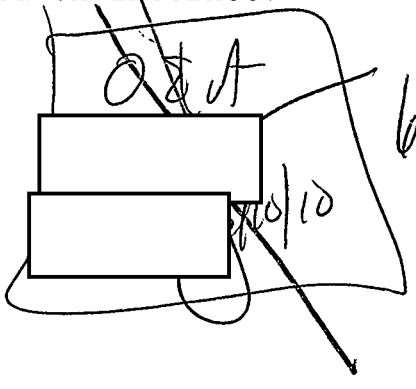
Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: Open and assign investigation.

Details: On 6/9/2010 security group GOATSE SECURITY, email address: security@goatse.fr, telephone number: (323)306-4576, exploited a vulnerability or security flaw in AT&T's protocols that has given them access to email addresses of over 114,000 iPad users.

When iPad 3G users sign up for a wireless data service with AT&T, the carrier detects the SIM's 19-digit ICC-ID, then asks for a contact email address. AT&T uses the email address to populate one of two log-in fields in the iPad's settings, so the users only ~~has~~ have to enter their password to check their account status.

GOATSE SECURITY, learned they could obtain an iPad user's email address, when given a unique SIM card identifier known ~~an~~ as ICC-ID (Integrated Circuit Card Identifier) present on every SIM card. Using a program on AT&T's website and guessing ICC-ID numbers, the hackers were able to download approximately 114,000 email addresses which they than posted on internet.



b6 b7C

To: Newark From: Newark
Re: [redacted] NEW, 06/10/2010 b3 b7E

Email addresses apparently belonging to New York Mayor Michael Bloomberg, top executives at Dow Jones, the New York Times Company, and Time Warner, were among those collected.

On 06/10/10, SA [redacted] contacted members of AT&T Security, located in Middletown, New Jersey, to enquire about the nature of the incident resulting from possible criminal activity of GOATSE SECURITY.

AT&T Security indicated the vulnerable files had been removed and it was no longer possible to replicate the incident and that an internal investigation was under way. No additional information was currently available, but AT&T Security indicated they would make an effort to locate the appropriate point of contact for the FBI to initiate discussions and would forward this information as soon as feasible. b6 b7C

Based on the above it is requested that a substantive case file be opened and assigned to the writer, and requested SA [redacted] be assigned as co-case agent.

To: Newark From: Newark
Re: [redacted]-NEW, 06/10/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

CYBER

AT CCU-2, DC

Read and clear.

♦♦

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired:

06/16/2010

Source from which Property Acquired:
FBI CART

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 1

WESTERN DIGITAL 1 TB HARDDRIVE.S/N WMATV6418627
CART IMAGED DRIVE OF MAC BOOK PRO LAPTOP S/N W88111F7YJX

Barcode: E4477516 Location:

06/16/2010

b3
b7E

Case Number: [redacted]
Owning Office: LITTLE ROCK

b6
b7C

[redacted]

1 - FILE
1 - PACKAGE

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH [redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 2

(1) ONE (1) SAMSUNG HARD DRIVE, SN: [redacted]
ITEM 1 ... (FOUND IN ROOM A - TUB IN CLOSET)

Barcode: E4477505 Location:

06/16/2010

Case Number: [redacted]

b3
b7E

Owning Office: LITTLE ROCK

b6
b7C

[redacted]

1 - FILE
1 - PACKAGE

Title and Character of Case:

[redacted]

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted] b6 b7C

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 3

(1) ONE (1) APPLE MINI-MAC COMPUTER, MODEL A1176, SERAIL NUMBER: [redacted] WITH POWER CABLE
ITEM 2 (FOUND IN ROOM C - KITCHEN BAR)

Barcode: E4477506 Location:

06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b3
b7E

[redacted] b6 b7C

1 - FILE
1 PACKAGE

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: Source from which Property Acquired:

06/15/2010 RESIDENCE SEARCH [redacted]

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted]

Description of Property: Date Entered

1B 4

(1) ONE (1) SD 256 MEMORY CARD
(2) ONE (1) MOTOROLA I425 CELL PHONE
(3) ONE (1) SAMSUNG SGH-T509 CELL PHONE, SN: [redacted]
(4) ONE (1) SAMSUNG SGH-807 CELL PHONE, SN:
ITEM 3 (FOUND IN ROOM A - GREEN TUB IN CLOSET)

Barcode: E4477507 Location: 06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b6
b7C

b3
b7E

[redacted]

FILE PACKAGE

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 5

(1) ONE (1) WESTERN DIGITAL HARD RIVE, 250 GB, MODEL WD2500JB, SN: [redacted]
ITEM 4 (FOUND IN ROOM A GREEN TUB IN CLOSET)

Barcode: E4477508 Location:

06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b3
b7E

b6
b7C

[redacted]

FILE PACKAGE

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: Source from which Property Acquired:

06/15/2010 RESIDENCE SEARCH [redacted]

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted]

Description of Property: Date Entered

1B 6

(1) ONE (1) KYOCERA CELL PHONE, MEIDCD: [redacted]
ITEM 5 (FOUND IN ROOM A - GREEN TUB IN CLOSET)

Barcode: E4477509 Location: 06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b3
b7E

b6
b7C

[redacted]

FILE
PACKAG

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 7

(1) ONE (1) BLACKBERRY 8830, ESN: [redacted]
PIN# [redacted]
ITEM 6 (FOUND IN ROOM A - GREEN TUB IN CLOSET)

Barcode: E4477510 Location:

06/16/2010

Case Number: [redacted]

b6
b7C

Owning Office: LITTLE ROCK

b3
b7E

[redacted]

FILE
PACKAG

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 8

(1) ONE (1) IPOD, MODEL A1136, SN: [redacted]
ITEM 7 (FOUND IN ROOM E - TOP OF BOOKCASE)

Barcode: E4477511 Location:

06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b3
b7E

b6
b7C

FILE
PACKAG

[redacted]

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: Source from which Property Acquired:

06/15/2010 RESIDENCE SEARCH [redacted]

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted]

Description of Property: Date Entered

1B 9

(1) ONE (1) APPLE MACBOOK WITH SN: [redacted]
ITEM 8 (FOUND IN ROOM E - BOOKCASE)

Barcode: E4477512 Location: 06/16/2010

Case Number: [redacted]
Owning Office: LITTLE ROCK

b3
b7E

b6
b7C

[redacted]

FILE
PACKAG

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 10

(1) ONE (1) APPLE LAPTOP A1286, SN: [redacted]
ITEM 9 (FOUND IN ROOM E - BED)

Barcode: E4477513 Location:

06/16/2010

Case Number: [redacted]

b6
b7C

Owning Office: LITTLE ROCK

b3
b7E

[redacted]

ILE
PACKAG

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: Source from which Property Acquired:
RESIDENCE SEARCH

06/15/2010 [redacted]

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted]

Description of Property: Date Entered
1B 11

(1) ONE (1) T-MOBILE CELL PHONE Q700, IMEI: [redacted]
ITEM 10 (FOUND IN ROOM E IN BLACK BACKPACK)

Barcode: E4477514 Location: 06/16/2010

Case Number: [redacted] b3 b6
Owning Office: LITTLE ROCK b7E b7C

[redacted]

ILE
PACKAG

Title and Character of Case:

[redacted]

b6
b7C

Date Property Acquired: 06/15/2010

Source from which Property Acquired: RESIDENCE SEARCH

[redacted]

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

Description of Property:

Date Entered

1B 12

(1) ONE (1) MACBOOK PRO, SN: [redacted]
ITEM 11 (FOUND IN ROOM E - FLOOR BY BED)

Barcode: E4477515 Location:

06/16/2010

Case Number: [redacted]

b3
b7E

Owning Office: LITTLE ROCK

[redacted]

b6
b7C

FILE
PACKAGE

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/11/2010

On June 10, 2010 and June 11, 2010, SA [redacted] conducted certain open-source investigations. [redacted] SA [redacted] used web searches and other documents to make the following observations:

b6
b7C
b7E

The investigation into recent hacking activity associated with the acquisition of 114,000 personal e-mail addresses for subscribers of the Third Generation (3G) service for the Apple iPad, which is supported and offered by AT&T, had revealed a possible subject of the name [redacted] Numerous open-source news articles, which began to appear after an article was posted on the media website gawker.com contained information crediting the incident to a group called GOATSE SECURITY. A visit to the GOATSE website, goatse.security.fr listed several members of the GOATSE team. [redacted]

SA [redacted] conducted a Google search on [redacted] which resulted in 310 hits for weblinks to documents references [redacted] Most of the links were to various versions of a document which identifies further online information about [redacted] The original post with this information appears to have been sent to an e-mail list which is hosted by, and archived at the site seclist.org. The title of the e-mail list was "Full Disclosure" and the message was titled [redacted]". The message content appeared to have been compiled by an individual named [redacted] and then posted by [redacted] with e-mail address [redacted] title for the document is [redacted] An informative dossier." According to that document, [redacted] has been known to use the online identities:

b6
b7C

[redacted]

Investigation on 06/11/2010 at [redacted] New Jersey

File # [redacted] Date dictated [redacted]

b3
b7E

by SA [redacted]

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] b3 b7E

[redacted] b6 b7C

According the GOATSE website, [redacted] confirms the use of [redacted] as his nicname and the link associated with his name on the GOATSE website points to a blog located at [redacted]

According to news articles, [redacted] and his team at GAOTSE were responsible for creating a script which perpetrated an "automated brute force" against a vulnerable website hosted by AT&T and used to register iPad customers. The script used, according to reports and interviews of [redacted] in days subsequent to the events, a recursive method to guess the Integrated Circuit Card Identifier (ICC-ID) for a specific iPad SIM. By sending these guessed ICC-ID's, the script retrieved and parsed the e-mail addresses of subscribers so those address were made available to GOATSE.

Additional searches for [redacted] provided links to articles in 2008 which refer to [redacted] causing havoc at marketplaces and provoking reactions in the cyber world."

Several of the articles mentioning [redacted] are attached and made part of this 302, including prints of the GOATSE website home page and the original GAWKER posted article.

Records checks and additional open-source research on [redacted] have provided the following identifying information:

[redacted]

[redacted]

b3
b7E

[redacted]

b6
b7C

Email
*[redacted]his
[redacted]-- he asks for paypal donations here too - to help support 'evangelistic efforts')
[redacted]

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2010

To: All Field Offices **Attn:** Cyber SSAs
Paris Legat Paris

From: Cyber Division
Cyber Criminal Section/CCU-2
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b3
b6
b7C
b7E

Case ID #: [redacted] (Pending) Serial 3

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: To notify all field offices that Newark Division has investigative lead on the AT&T/iPad matter.

Details: On 6/9/2010, a known hacker security group, Goatse Security, allegedly exploited a vulnerability in AT&T protocols and gained access to e-mail addresses for over 114,000 iPad users. Based on open source reporting, several offices initiated investigative efforts into this matter. After reviewing various factors, such as venue and Newark's proximity to the victim company, Cyber Division determined Newark Division will be the Originating Office (OO) on this investigation.

Cyber Division hereby directs all field offices which have initiated an investigation or served legal process pertaining to this matter to coordinate with Newark Division, Cyber Squad SSA [redacted]

b6
b7C
b7E

UNCLASSIFIED

To: All Field Offices From: Cyber Division
Re: [redacted] 06/11/2010

b3
b7E

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

All field offices which initiated assessments or investigations are requested to close their respective investigation or assessment and forward all pertinent information to Newark Division.

♦♦

[redacted]

From: [redacted]
Sent: Thursday, June 10, 2010 1:50 PM
To: [redacted]
Subject: Preservation request for iPad breach information

[redacted]

This email is to follow-up on our conversation this afternoon. The FBI is investigating the facts surrounding the possible data breach affecting some iPad users that [redacted] ecently reported. The FBI requests that [redacted] preserve all relevant information related to this incident.

b6
b7C
b7E

Please confirm that the below contact information is correct and provide a fax number for additional correspondence.

[redacted]

Thank you for your cooperation.

SSA [redacted] Unit Chief
Federal Bureau of Investigation
Cyber Division
Washington, DC
202/324-3000

[redacted] 4

b3
b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/10/2010

On Thursday, June 10, 2010 at around midday, Supervisory Special Agent (SSA) [redacted] telephonically contacted [redacted] of Gawker Media, LLC, 210 Elizabeth Street, 4th Floor, New York, New York, 10012, [redacted] SSA [redacted] identified himself and explained that the purpose of his call was to notify Gawker Media that the Federal Bureau of Investigation was investigating the facts surrounding the possible data breach affecting some iPad users. Gawker Media had recently published an article about the incident on it's VALLEYWAG blog.

[redacted] advised that Gawker Media had received the list of email addresses and corresponding iPad integrated circuit card identifiers (ICC-IDs) as well as the software code that the responsible individual used to obtain the list. SSA [redacted] requested Gawker Media preserve all information it had related to the incident and that no further sensitive AT&T and/or Apple customer information be published. [redacted] advised that no sensitive information had been published to date, only redacted exemplars, and that Gawker Media was only reporting the facts of the story.

b6
b7C

SSA [redacted] followed up with an email to [redacted] at 1:50 p.m., which will be separately serialized to the case file. SSA [redacted] advised [redacted] that a formal preservation request on letterhead would be forthcoming.

Investigation on 06/10/2010 at New York, New York (telephonically)

File [redacted] Date dictated [redacted]

by SSA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2010

[redacted] date of birth [redacted] social security account number [redacted] home address [redacted] and cellular telephone [redacted] was advised of the identity of the interviewing Agent and the purpose of the interview. The interview started on [redacted] at his residence, and shortly thereafter moved to the investigating Agent's assigned Government vehicle. [redacted] provided the following information:

[redacted]

[redacted]

[redacted]

heard of Goatse Security in an online Forbes article. According to the article, Goatse Security was involved in a recent incident involving AT&T and IPads. Someone on Twitter recommended he look there. could not recall who gave him the recommendation, but said it might have been The article to which referred indicated affiliated with Goatse Security.

When asked to more fully describe the AT&T/IPad matter, said he thought a significant number of emails involving AT&T/IPads were leaked. was unsure of Goatse Security's role in the AT&T/IPad incident.

recalled reading an article about the AT&T/IPad matter, similar to the one in Forbes, in the Wall Street Journal. thought the Wall Street Journal article also linked to the AT&T/IPad incident, but could not remember for sure, as he does not remember his Internet habits very well.

seemed pretty happy the past few days.

has not seemed angry toward large telecommunication companies like AT&T and Apple.

According to "Gawker" is a technology blog. thought he read in the Forbes article that Gawker had information about the AT&T/IPad incident.

first heard of exploits against AT&T/IPad when he read about the incident in Forbes.

has heard but he does not recall the specifics of comments. has never heard say he intended to harm any groups of people. does not have any guns at was unsure whether has guns elsewhere.

b3
b6
b7C
b7E

[redacted] on [redacted] is unaware of any groups of which [redacted] is a member.

Later, during a brief follow-up interview [redacted] is a member of the Internet group, [redacted] only knew the first letter in [redacted] said he did not know much about the group. b3 b6 b7C b7E

A couple years ago, [redacted] fabricated a claim that [redacted]

After reading the aforementioned Forbes and Wall Street Journal articles about Goatse Security and AT&T, [redacted] believes he still does not know enough information about [redacted] activities to conclude he was involved in computer hacking activities.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2010

[redacted] Date of Birth (DOB): [redacted]
Social Security Number (SSN): [redacted], was interviewed by SA [redacted] The interview took place subsequent to the execution of a Federal Search warrant. [redacted] was advised of the identities of the interviewing agents and the nature of the interview. She provided the following information:

[redacted]

b3
b6
b7C
b7E

[redacted] had several jobs, periodically, while in California. [redacted]

[redacted]

Investigation on 06/15/2010 at Fayetteville, Arkansas

File # [redacted] Date dictated _____

by [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302a (Rev. 10-6-95)

[redacted]

b3
b6
b7C
b7E

Continuation of FD-302 of [redacted], On 06/15/2010, Page 2

[redacted]

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 06/17/2010

To: Newark

From: Newark
FT2
Contact:

Approved By:

Drafted By:

Case ID #: (Pending) -8

Title: ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: To document the authorization for use of rental vehicle as operational necessity during travel.

Details: On June 15, 2010, writer and SA traveled to Fayetteville, Arkansas for execution of a Federal Search Warrant in the captioned matter. Fayetteville is within the AOR of the Fayetteville RA of the Little Rock Division. No government vehicle was available for transportation during the period of travel for Newark SAs. In addition, public transport was not readily available for travel between the airport and hotel accommodations. As such, SA contacted SSA to confirm authority to use a rental vehicle. SSA advised via e-mail of concurrence on necessity of rental vehicle due to expediency of the warrant.

♦♦

UNCLASSIFIED

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 06/17/2010

To: Little Rock **Attn:** Evidence Tech
Newark **Attn:** Evidence Tech

From: Newark
FT2
Contact:

Approved By:

Drafted By:

Case ID #: (Pending) -9

Title: ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: To request evidence be transferred to Newark division.

Details: On June 15, 2010, writer and SA with the assistance of FBI Little Rock, Fayetteville RA executed a federal search warrant, authorized by the Western District of Arkansas. During the search, items were seized and processed as per FBI procedure in the Little Rock Division. Newark is requesting these items, specifically through be transferred to Newark Evidence Control.

UNCLASSIFIED

To: Little Rock From: Newark
Re: [redacted] 06/17/2010

b3
b7E

LEAD(s):

Set Lead 1: (Action)

LITTLE ROCK

AT LITTLE ROCK, ARKANSAS

Little Rock evidence technician is requested to transfer all evidence in captioned investigation to Newark evidence technician.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/21/2010

To: Newark

From: Little Rock
Squad 7/ Fayetteville RA
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) - 10

Title: [redacted] ET AL;
dba GOATSE SECURITY;
COMPUTER INTRUSION- CRIMINAL

b3
b6
b7C
b7E

Synopsis: Send 1As to Newark.

Enclosure(s): (3) 1A envelopes containing search related documents from the search of [redacted]

Details: (3) 1A envelopes are enclosed containing search documents and CDs containing photos from the search of [redacted] on 6/15/2010.

S:\DRAFTS\7\[redacted]179[redacted]03.ec.wpd

b6
b7C

UNCLASSIFIED

To: Newark From: Little Rock
Re: [redacted] 06/21/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

NEWARK

AT NEWARK, NEW JERSEY

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/16/2010

On June 15, 2010 agents from the Federal Bureau of Investigation, Newark Division, with the assistance of FBI Little Rock, Fayetteville RA, executed a federal search warrant at the residence of subject [redacted] located at [redacted] In addition to Newark Special Agents (SAs) [redacted] the following Fayetteville/Little Rock personnel were involved with the search:

Fayetteville RA, Little Rock Division
SA [redacted]
TFO
SA
SA
SA
SA
SA
SA

b6
b7C

Fayetteville Police Department
Officer [redacted]

CART
FE [redacted]
FE
FE

The warrant was executed at 7:43 AM. Immediately on entry, Agents and Officers encountered resident [redacted] Resident [redacted] were in a loft within the residence [redacted] appeared at the top of the stairs as agents approached the base of the stairs. [redacted] was not immediately visible, but was revealed by [redacted] upon questioning from agents. [redacted] was called from the loft and both [redacted] and [redacted] along with [redacted] were secured. The house was declared secure at 7:45 AM.

After the loft area was cleared, SAs [redacted] entered the southern room of the loft and discovered a cable modem and wireless network router. SA [redacted] unplugged the cable

---

Investigation on 06/15/2010 at Fayetteville, AR

File # [redacted] -12 MC Date dictated Not Dictated

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

supplying network connectivity to the cable modem, but left both the cable modem and the wireless router active.

SAs [redacted] next entered the bedroom area of the northern room of the loft where [redacted] were located at contact. Upon entry, SA [redacted] observed an open and running Apple Macintosh Laptop computer displaying a command shell. SA [redacted] observed the shell displayed contained commands "rm -rf /" This command was entered multiple times, with the last entry appearing to be in a running state. Recognizing this series of commands as an attempt to erase the contents of the computer, SA [redacted] initiated a "control - c" key stroke to halt the process. SA [redacted] next entered the command "pwd" to show the current working directory for the shell followed by an "ls" command to list files. SA [redacted] observed that both commands ran and performed the expected function. The current working directory was the user directory for user [redacted] command listed numerous files. Based on this observation, SA [redacted] believed the previous attempted "rm -rf /" command was unsuccessful. b6 b7C

At 7:51 AM, CART Field Examiners began working on imaging and duplication of files located on systems discovered in the search of the loft bedroom. SAs [redacted] began interviewing [redacted] SA [redacted] and TFO [redacted] began interviewing [redacted] and SAs [redacted] began interviewing [redacted]

At approximately 9:27 AM, the interview with [redacted] was concluded at his request in order to contact his attorney. Details of the interview with each resident are located in separate FD-302s.

At the conclusion of the interview, SAs [redacted] removed [redacted] to the lower level of the residence and requested his attorney's number so as to contact the attorney for him. [redacted] indicated he did not know the attorney's number nor did he recall the attorney's name beyond a first name of [redacted] indicated the attorney's number was located in [redacted] telephone, which was in the process of duplication with CART at that time. b6 b7C

At 10:05 AM, SA [redacted] scrolled through [redacted] phone in the presence of both [redacted] The attorney's number was located and a call was placed for [redacted] was unable to reach the attorney and requested an

additional call to another attorney, [redacted] was unable to reach this attorney as well and left a voice-mail message.

During the period when phone calls were being placed, agents and officers searched the loft area where [redacted] had been interviewed. The search revealed a plastic bag containing numerous items which appeared to be controlled substances. [redacted] was shown the contents of the bag and asked what they were. He indicated they were his drugs. When asked if he was covering for others in the residence by responding as such, [redacted] again stated they were his drugs.

At that point, [redacted] was detained and told he was being held until members of the Drug Task Force could arrive to determine if he would be arrested. At approximately 10:20 AM, Detectives [redacted] from the Arkansas 4th Judicial District Drug Task Force arrived to examine the suspected drugs. At 11:15 AM, [redacted] was placed in custody and escorted from the residence by Fayetteville PD. b6 b7C

During CART examination, the on-scene imaging of the system belonging to [redacted] failed. [redacted] who had left the residence, was contacted via cell phone and notified his laptop would be taken from the residence for an attempt at re-imaging by CART FE [redacted] during the evening at the Fayetteville RA. A separate FD597 was completed and presented to [redacted] to provide to [redacted] The imaging of this system is documented in a separate serial to this file. The FD597 for receipt of [redacted] laptop was placed in a 1A and submitted to the file.

At 4:05 PM CART examination was completed.

At 4:14 PM, [redacted] was provided with a copy of the FD597 showing the items which were to be seized and allowed to confirm each item.

At 4:17 PM, exit photos were taken and the scene was released to [redacted] at 4:24 PM.

A list of the items seized is as follows:

Samsung HDD serial #: [redacted]
Apple Mac Mini, serial # [redacted]
256MB SD card

[redacted] b3 b7E

Motorola i425 cell phone, (no serial #)
Samsung T509 cell phone, serial #: [redacted]
Samsung 807 cell phone, serial #: [redacted]
Western Digital HDD, serial #: [redacted]
Kyocera cell phone, serial #: [redacted]
Blackberry 8830 cell phone, ESN: [redacted]
iPod, serial #: [redacted]
Apple Macbook, serial # [redacted]
Apple Laptop, serial #: [redacted]
T-Mobile cell phone, IMEI: [redacted]
Apple Macbook Pro, serial [redacted]

All search logs and documentation, including the FD597 which [redacted] signed were collected and processed by SA [redacted] b6 b7C [redacted] and will be forwarded to Newark in an official communication.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 06/28/2010

To: Little Rock **Attn:** Evidence Tech
Newark **Attn:** Evidence Tech

From: Newark
FT2
Contact:

Approved By:

Drafted By:

Case ID (Pending) -13

Title: ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: To request Derivative Evidence Items be transferred to Newark division.

Details: On June 15, 2010, writer and SA with the assistance of FBI Little Rock, Fayetteville RA executed a federal search warrant, authorized by the Western District of Arkansas.

b3
b6
b7C
b7E

During the search, CART created derivative evidence items (DE) have been submitted to Little Rock evidence control, and assigned 1B14.

Newark is requesting these items, specifically be transferred to Newark Evidence Control.

UNCLASSIFIED

To: Little Rock From: Newark
Re: [redacted] 06/28/2010

b3
b7E

LEAD(s):

Set Lead 1: (Action)

LITTLE ROCK

AT LITTLE ROCK, ARKANSAS

Little Rock evidence technician is requested to transfer all evidence in captioned investigation to Newark evidence technician.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2010

On Thursday, June 10, 2010 at approximately 10:00 a.m., Executive Assistant Director (EAD) Chad Fulgham, Assistant Director (AD) Gordon Snow, Supervisory Special Agents (SSAs) [redacted] all with the Federal Bureau of Investigation (FBI), attended a meeting with [redacted] AT&T Government Solutions. The meeting was held in EAD Fulgham's office in the J. Edgar Hoover Building in Washington, DC. Joining the meeting via teleconference from AT&T included [redacted] and perhaps others unknown. Collectively, the AT&T representatives advised as follows:

AT&T recently experienced a security incident involving the newly released Apple iPad. An individual from Goatse Security who goes by the handle [redacted] wrote a script that ran a large number of possible iPad integrated circuit card identifier (ICC-ID) numbers against an AT&T authentication website. As a convenience feature, when a previously registered iPad connects to the site, the site would recognize the ICC-ID number and pre-populate the registrant's email address in a field. The script was designed to harvest each email address as it was returned. As the iPad was only recently released, the list of registrants included early adopters and other notable people, including high level government officials. b6 b7C

According to AT&T, [redacted] noticed some email addresses on the list for individuals employed by the Reuters news organization. [redacted] contacted the Reuters employees to notify them of the iPad vulnerability, intending for Reuters to write a news story. When Reuters did not do as he wished, [redacted] took the information to the blog site Gawker, who quickly published an article.

AT&T is working to document its loss as a result of the incident.

Investigation on 06/10/2010 at Washington, DC

File # [redacted] -14 Date dictated [redacted]

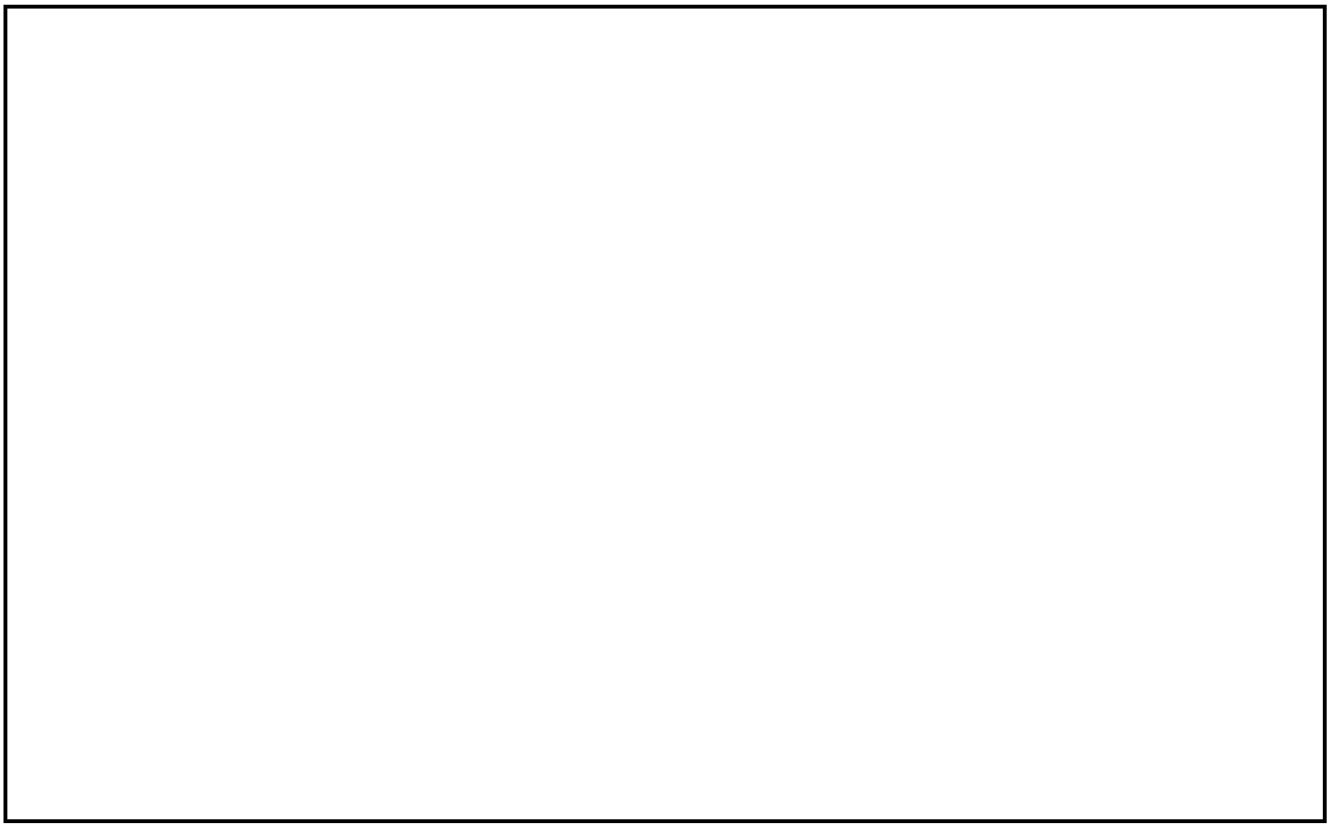
by SSA [redacted] SSA [redacted] b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FT2

b6
b7C

b6
b7C
b7E



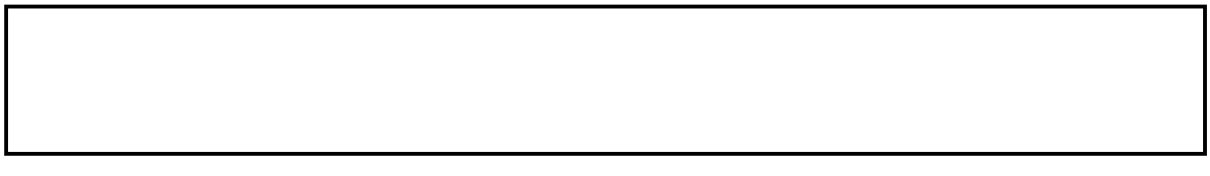
On June 14, 2010, a Federal Search Warrant was issued in the Western District of Arkansas for the search of the residence of [redacted] described above and detailed below.

Beginning on June 9, 2010, news reports surfaced indicating a hacking group known as "Goatse Security" had discovered a vulnerability in one of the websites established to manage the AT&T 3G subscriptions for the Apple iPad. According to reports, Goatse had exploited the vulnerability and provided online media outlet Gawker with approximately 114,000 e-mail addresses along with the unique ID (ICC-ID) of iPad 3G subscribers.

Within two days, an individual identifying himself as [redacted] had been interviewed by several media outlets and during these interviews, claimed responsibility for the AT&T breach and the subsequent release of the data to the media outlet, Gawker. [redacted] was also reported as having provided to the media a copy of the script used to obtain the data from AT&T's files.

b6
b7C
b7E

Based on FBI Investigations, [redacted] was identified as [redacted] In addition to the [redacted] alias, [redacted] uses numerous online aliases and phony names for appearances at hacker conventions.



FEDERAL BUREAU OF INVESTIGATION

OTHER Sealed per Court Order

Date of transcription 07/06/2010

[redacted]

Writer received response, [redacted] Writer placed a copy of the response [redacted] into an FD-340 (1A) envelope, to be maintained with the main case file in this matter.

A copy of [redacted] has been also been placed into an FD-340 (1A) envelope to be maintained with the main case file in this matter.

Investigation on 07/06/2010 at Somerset, NJ

File # [redacted]-16 Date dictated 07/06/2010

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-542 (Rev. 03-23-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/25/2010

To: Newark **Attn:** SSA [redacted]

From: Newark
FT2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) (Pending)

Title: [redacted], ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: To claim statistical accomplishments for investigative techniques.

Details:

On June 10, 2010 agents from the Federal Bureau of Investigation, Newark Division, discovered a script titled, "iPad 3G Account Slurper", in open source documents, believed to be used to steal emails addresses from AT&T for iPad 3G users.

On June 15, 2010 agents from the Federal Bureau of Investigation, Newark Division, with the assistance of FBI Little Rock, Fayetteville RA, executed a federal search warrant at the residence of [redacted] located at [redacted]

As such, writer claims 4 stats and SA [redacted] claims 4 stats.

b6
b7C
OTHER Sealed per Court Order

UNCLASSIFIED

To: Newark From: Newark
Re: [redacted] 06/25/2010

b3
b6
b7C
b7E
OTHER Sealed per Court Order

Accomplishment Information:

Number: [redacted]
Type: [redacted]
ITU:
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

Number: 1
Type: CIP SUBJECT INTERVIEWED
ITU: AGENT INTERVIEW
ITU: CART
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

Number: 1
Type: CIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: AGENT INTERVIEW
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

To: Newark From: Newark
Re: [redacted] 06/25/2010

b3
b6
b7C
b7E
OTHER Sealed per Court Order

Number: [redacted]
Type: [redacted]
ITU: [redacted]
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

Number: 1
Type: CIP SUBJECT INTERVIEWED
ITU: AGENT INTERVIEW
ITU: CART
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

Number: 1
Type: CIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: AGENT INTERVIEW
ITU: LIAISON WITH OTHER AGENCY
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: FT2

♦♦

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

100 Davidson Avenue
Suite 209
Somerset, New Jersey 08873
July 13, 2010

[redacted]

b3
b6
b7C
b7E

Dear Custodian of Records:

You are hereby requested, under the provisions of Title 18, United States Code, Section 2703(f), to "...take all necessary steps to preserve records and other evidence in [your] possession pending issuance of a court order or other process" relating to the below listed domains the following records in your custody or control, including any records stored on backup media:

[redacted]

You are requested to preserve for a period of 90 days the records described above currently in your possession. This request applies only retrospectively; it does not obligate you to capture and preserve new information that arises after the date of this request.

You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. Any

[redacted] /F

such disclosure could subject you to criminal liability for obstruction of justice. If compliance with this request may result in permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such action.

Please refer any questions to Special Agent [redacted] FBI, Newark Division, Franklin Township Resident Agency, telephone [redacted] Thank you for your cooperation. b6 b7C b7E

Sincerely,

Michael Ward
Special Agent In Charge

By: [redacted]
[redacted]
Supervisory Special Agent

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/18/2010

On June 15, 2010, during the execution of a Federal Search Warrant, authorized in the Wester District of Arkansas, located at the [redacted] Special Agent (SA) [redacted] conducted the following investigation:

During the clearing of the residence, a cable modem, serial number [redacted] MAC address [redacted] was located and disconnected from the cable service. However, the cable modem was left powered on and connected to a Cisco/Linksys WRT54G2 v1 wireless router which was also left powered on. The Linksys router had a serial number of [redacted] and an external interface MAC address of [redacted]

While the search was being conducted, at 11:29AM, SA [redacted] provided by CART Field Examiner (FE) [redacted] at this time. SA [redacted]

b6
b7C
b7E

SA [redacted] initiated a [redacted]

At 11:35AM, SA [redacted] SA [redacted] was presented with [redacted] SA [redacted] was able to [redacted] were as follows:

Investigation on 06/15/2010 at Fayetteville, Arkansas

File # [redacted] -21 Date dictated N/A

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

b3
b6
b7C
b7E

[redacted]

At 11:42AM, SA [redacted]

[redacted] SA [redacted]

[redacted]

[redacted]

At 11:44AM, SA [redacted]

[redacted]

At 11:46AM, SA [redacted]

[redacted]

[redacted]

b3
b6
b7C
b7E

[redacted]

At 11:49AM, SA [redacted]

[redacted]

CART FE [redacted] assisted in the above investigative activity by [redacted] produced by CART FEs on scene (and detailed in other reports) were burned to a DVD and provided to SA [redacted] SA [redacted] placed the DVD in a 1A envelope and submitted to the file.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/29/2010

To: Newark **Attn:** SA

From: Little Rock
Squad 6
Contact: FE

Approved By:

Drafted By:

Case ID # (Pending) -22

Title: ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: Request for CART search assistance in this matter has been completed.

Enclosure(s): Enclosed for Newark are the following items:
1) an FD-340 containing the original notes from the initial CART search assistance.
2) a Report of Examination containing results of the CART search assistance.

Details: On June 15, 2010, FE FE and FET assisted in the execution of a search warrant at The enclosed documentation provides details regarding the CART search assistance.

b6
b7C

♦♦

UNCLASSIFIED

180 02.ec

b6
b7C

To: Newark From: Little Rock
Re: [redacted] 06/29/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

Newark

AT Newark, NJ

Read and clear.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/16/2010

To: Newark **Attn:** SA

From: Indianapolis
C7
Contact: SA

b3
b6
b7C
b7E

Approved By:

Drafted By: (C7\197 02.ec)

Case ID #: 24 (Pending)

Title: ET AL;
D/B/A/GOATSE SECURITY
COMPUTER INTRUSION - CRIMINAL

b7D

Synopsis: Source Reporting Documentation from CHS

Enclosure(s): FD-1023s dated 06/10/2010 and 7/9/2010 with their respective 1A envelopes.

Details: CHS provided information pertinent to captioned case. FD-1023s and respective 1A envelopes with information obtained from CHS are enclosed for submission into the paper copy of . Electronic versions of enclosed FD-1023s have been uploaded into ACS/Sentinel. Unredacted copies of supplied documents are being maintained in the CHS file and by the drafter.

b3
b7D
b7E

UNCLASSIFIED

b3
b7E

To: Newark From: Indianapolis
Re: [redacted] 07/16/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

NEWARK

AT NEWARK

Read and clear.

♦♦

Record Request
FD-125 (Rev. 4-1-93)

Date 7/27/2010

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

To	Buded
IOA [redacted] FTRA	
Retur [redacted] SA	File Number [redacted] -26

Name and aliases of subject, applicant, or employee, and spouse

[redacted]

Address
Residence _____
Business _____
Former _____
_____

b3
b6
b7C
b7E

* Date and place of marriage (if applicable) _____

Race	Sex	Age	Height	Weight	Hair	Eyes
	☐ Female ☐ Male					

Birth date	Birthplace	
Arrest Number	Fingerprint classification	Criminal specialty

Social Security Number	Drivers License Number ☐ D/L Photo ☐ Other

Specific information desired NCIC, postal, DL info

Results of check

Read & Approved

[redacted]

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/29/2010

To: San Francisco **Attn:** CY-1
SA [redacted]
Attn: Evidence Control
ECT [redacted]

Newark **Attn:** Evidence Control
ECT [redacted]

From: Newark
FT2
Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) -31

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

Synopsis: To request transfer of evidence.

Details: Newark requests evidence items 1B15 through 1B38 (inclusive) of the captioned investigation, currently in Oakland evidence control, be transferred to Newark for forensic examination and review.

UNCLASSIFIED

To: San Francisco From: Newark
Re: [redacted] 07/29/2010

LEAD(s):

Set Lead 1: (Action)

b3
b7E

SAN FRANCISCO

AT OAKLAND

Oakland evidence control is requested to transfer the items listed for [redacted] currently in custody of Oakland, to Newark's Evidence Control.

♦♦

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

100 Davidson Ave
Suite 209
Somerset, New Jersey 08873
(732) 302-2921
July 27, 2010

[redacted]

b3
b6
b7C
b7E

You are hereby requested, under the provisions of Title 18, United States Code, Section 2703(f), to "... take all necessary steps to preserve records and other evidence in [your] possession pending issuance of a court order or other process" relating to the account using [redacted] This is to include the following records in your custody or control, including records stored [redacted]

[redacted]

[redacted] -32

[redacted]

You are hereby requested to preserve for a period of 90 days the records described above currently in your possession. This request applies only retrospectively; it does not obligate you to capture and preserve new information that arises after the date of this request.

You are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. Any such disclosure could subject you to criminal liability for obstruction of justice. b6 b7C b7E

Please refer any questions to Special Agent [redacted] Federal Bureau of Investigation, Newark Division, Franklin Township Resident Agency, telephone number [redacted] Thank you for your cooperation.

Sincerely,

Michael B. Ward
Special Agent in Charge

[redacted]
Supervisory Special Agent

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/19/2010

To: San Francisco **Attn:** SAC San Francisco

Squad CY1
SSA [redacted]

From: Newark
FT2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) -34

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

Synopsis: To request SAC approval for travel and investigative assistance for San Francisco.

Details: The captioned subject and his associates comprise a sub-group of an Internet trolling group known as the "GAY NIGGER ASSOCIATION OF AMERICA" (GNAA). The GNAA was established, as per its own reference, as an online organization of individuals with the goal of creating posts and other "mayhem" on the web for the purpose of causing discomfort. GNAA activities include the posting of crude photos and references in comment sections on websites, sending e-mails and other communications to "targets" the group has determined to have offended them, and other such harassing actions.

A subset of the GNAA has chosen to define itself as GOATSE SECURITY and post online information purporting the group to be an Internet security research organization. GOATSE claims to have discovered a cross-protocol scripting vulnerability which allows them to hijack a browser and use it as a proxy for other non-web browsing activity (such as VoIP telephone calls). The name GOATSE was taken from an online shock image which is

To: San Francisco From: Newark
Re: [redacted] 07/19/2010

intended to disturb recipients who receive it. Chats and communications, obtained during the captioned investigation, indicate members of GOATSE were reveling in the use of the term in the main stream media as if this were somehow a private joke. An interview of GOATSE member [redacted] conducted during a search of his residence on 6/15/10 provided similar information concerning the choice of the name GOATSE.

Additional evidence recovered during that search further indicates the name of GOATSE was chosen as an "inside joke" between GNAA members in an effort to "prank" the media via repeated use of the term. An FBI source has further provided that [redacted] suggested, during the execution of the scripted intrusion at AT&T, that this could be "big media news".

During an IRC chat session, GOATSE member [redacted] b3 b6 b7C b7E

Newark's investigation has shown that [redacted] is likely: [redacted]

Newark is requesting initial assistance from FBI San Francisco in positively identifying [redacted] and providing intelligence for use in a search warrant. Further, Newark is requesting San Francisco assist in the execution of a forthcoming search warrant and coordinate with Newark on same. Newark is requesting SAC authority for two agents to travel to San Francisco to coordinate this action from 07/25/2010 until 07/28/2010. Newark is requesting this authority be granted in anticipation of the need for specific case knowledge for conducting searches as well as interviews.

To: San Francisco From: Newark
Re: [redacted] 07/19/2010

b3
b6
b7C
b7E

LEAD(s):

Set Lead 1: (Action)

SAN FRANCISCO

AT SAN FRANCISCO

Newark is requesting San Francisco assist in the identification and determination of residence for:

[redacted]

Newark is further requesting San Francisco coordinate with SA [redacted] (cell), in anticipation of execution of legal process at the [redacted] residence on 07/27/2010.

Please do not contact [redacted] directly at this time.

Finally, Newark is requesting San Francisco provide SAC authorization for travel as detailed in this communication.

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/28/2010

To: Newark **Attn:** SA

From: Indianapolis
C7
Contact: SA

Approved By:

Drafted By: (C7\209 01.ec)

Case ID # 36 (Pending)

Title: ET AL;
D/B/A/GOATSE SECURITY
COMPUTER INTRUSION - CRIMINAL

Synopsis: Source Reporting Documentation from CHS

Enclosure(s): Three FD-1023s dated 07/21/2010 with 1A envelopes.

Details: CHS provided information pertinent to captioned case. FD-1023s and their respective 1A envelopes, which contain subject identification information obtained from CHS are enclosed for submission into the paper copy of Note the documents contained within the 1A envelopes have been redacted. Electronic versions of enclosed FD-1023s have been uploaded into the electronic case file of Unredacted copies of supplied documents are being maintained in the A folder of the source file for

b3
b6
b7C
b7E

b3
b7D
b7E

UNCLASSIFIED

36

b3
b7E

To: Newark From: Indianapolis
Re: [redacted] 07/28/2010

b3
b7E

LEAD(s):

Set Lead 1: (Info)

NEWARK

AT NEWARK

Read and clear.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/26/2010

On July 22, 2010, FBI San Francisco requested the California Employment Development Department (EDD), located at 801 Turk Street, San Francisco, California, to provide employment information regarding [redacted] EDD responded to FBI San Francisco's request on July 23, 2010 and provided the following employment information on [redacted]

b6
b7C

Employer: [redacted]

Address [redacted]

Phone: [redacted]

EDD's response has been placed in a 1A envelope.

Investigation on July 23, 2010 at Oakland, California

File # [redacted]-38 Date dictated July 26, 2010

by [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/20/2010

To: [redacted] **Attn:** SA [redacted]

From: Newark
FT2
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) 39

Title: [redacted] ET AL;
D/B/A GOATSE SECURITY;
COMPUTER INTRUSION - CRIMINAL

b3
b6
b7C
b7E

GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(e)

Synopsis: To set lead for service of Federal Grand Jury (FGJ) Subpoena.

Details: [redacted] has been identified as an individual in possession of information pertinent to the captioned investigation. As such, the USAO of the District of New Jersey has issued the enclosed FGJ Subpoena to be served on [redacted] at the address provided in the subpoena.

b3
b6
b7C

The Subpoena is requesting the presence of [redacted] before the Grand Jury on [redacted] As such, writer contacted SA [redacted] and provided a scanned copy of the Subpoena for service as soon as possible to allow time for [redacted] with the USAO in the District of New Jersey. No hard copy of the subpoena is being enclosed with this communication.

UNCLASSIFIED

To: [redacted] From: Newark
Re: [redacted] 08/20/2010

b3
b6
b7C
b7E

LEAD(s):

Set Lead 1: (Action)

[redacted]

AT [redacted]

Serve the previously provided FGJ Subpoena on [redacted] at the address:

[redacted]

[redacted] should also be instructed to contact AUSA [redacted] as addressed on the Subpoena for arrangements [redacted] to appear before the Grand Jury.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION OTHER sealed per court order b6 b7C

Date of transcription 08/23/2010

On August 13, 2010, SA [redacted] obtained a Federal Search Warrant, authorized in the District of New Jersey, pursuant to 18 USC 2703 by U.S. Magistrate Judge Esther Salas. The warrant was served on [redacted] The warrant sought [redacted]

On August 20, 2010, SA [redacted] received [redacted] from [redacted] requested in the warrant. A copy of the warrant, as well as the affidavit and application and the sealing order were placed in the substantive file. The DVD-R disks were duplicated for working copies and the originals were placed in a 1A envelope and submitted to the file.

Investigation on 08/20/2010 at Somerset, New Jersey

File # [redacted] 40 Date dictated N/A

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.